

Helsinki 18.9.2000

10/030538

10/01 468

4

F100/640

ETUOIKEUSTODISTUS  
PRIORITY DOCUMENT



Hakija  
Applicant

Nokia Telecommunications Oy  
Helsinki

Patenttihakemus nro  
Patent application no

991597

Tekemispäivä  
Filing date

12.07.1999

Kansainvälinen luokka  
International class

H04Q

Keksinnön nimitys  
Title of invention

"Access context management for macro level mobility management registration  
in an access network"

(Access-kontekstin hallinta makrotason liikkuvuudenhallintarekisteröinnin  
yhteydessä access-verkoissa)

Hakijan nimi on hakemusdiaariin 05.12.1999 tehdyn nimenmuutoksen  
jälkeen **Nokia Networks Oy**.

The application has according to an entry made in the register  
of patent applications on 05.12.1999 with the name changed into  
**Nokia Networks Oy**.

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä  
patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä,  
patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the  
description, claims, abstract and drawings originally filed with the  
Finnish Patent Office.

*Marketta Tehikoski*

Marketta Tehikoski  
Apulaistarkastaja

Maksu 300,- mk  
Fee 300,- FIM

Osoite: Arkadiankatu 6 A Puhelin: 09 6939 500 Telefax: 09 6939 5328  
P.O.Box 1160 Telephone: + 358 9 6939 500 Telefax: + 358 9 6939 5328  
FIN-00101 Helsinki, FINLAND

BEST AVAILABLE COPY

## Access context management for macro level mobility management registration in an access network

### Field of the Invention

The invention relates to a management of access context in an access network, in connection with a macro level mobility management registration, such as a Mobile IP registration.

### Background of the Invention

Mobile communications system refers generally to any telecommunications system which enable a wireless communication when users are moving within the service area of the system. A typical mobile communications system is a Public Land Mobile Network (PLMN). Often the mobile communications network is an access network providing a user with a wireless access to external networks, hosts, or services offered by specific service providers.

The general packet radio service GPRS is a new service in the GSM system (Global System for Mobile communication). A subnetwork comprises a number of packet data service nodes SN, which in this application will be referred to as serving GPRS support nodes SGSN. Each SGSN is connected to the GSM mobile communication network (typically to a base station controller BSC or a base station BTS in a base station system) so that the SGSN can provide a packet service for mobile data terminals via several base stations, i.e. cells. The intermediate mobile communication network provides a radio access and a packet-switched data transmission between the SGSN and mobile data terminals. Different subnetworks are in turn connected to an external data network, e.g. to a public switched data network PSPDN, via GPRS gateway support nodes GGSN. The GPRS service thus allows to provide packet data transmission between mobile data terminals and external data networks when the GSM network functions as a radio access network RAN.

Third generation mobile systems, such as Universal Mobile Communications system (UMTS) and Future Public Land Mobile Telecommunications system (FPLMTS), later renamed as IMT-2000 (International Mobile Telecommunication 2000), are being developed. In the UMTS architecture a UMTS terrestrial radio access network, UTRAN, consists of a set of radio access networks RAN (also called radio network subsystem RNS) connected to the core network (CN). Each RAN is responsible for the resources of its set of

cells. For each connection between a mobile station MS and the UTRAN, one RAN is a serving RAN. A RAN consists of a radio network controller RNC and a multiplicity of base stations BS. One core network which will use the UMTS radio access network is the GPRS.

5 One of the main targets in the development of mobile communication network is to provide IP (Internet Protocol) service with a standard IP backbone which would use a combination of mobile network mobility management in the mobile networks and Mobile IP. The basic IP concept does not support the mobility of the user: the IP addresses are assigned to network interfaces in dependence on their physical location. In fact, the first field of an IP address (the NETID) is common to all interfaces that are linked to the same Internet subnet. This scheme prevents the user (the mobile host) from keeping its address while moving over different Internet subnets, i.e. while changing the physical interface.

10 In order to enhance the mobility in the Internet a Mobile IP protocol for IP version 4 have been introduced by the Internet Engineering Task Force (IETF) in the standard RFC2002. Mobile IP enables the routing of IP datagrams to mobile hosts, independently of the point of attachment in the sub-network. The mobile IP protocol introduces following new functional or architectural entities.

15 'Mobile Node MN' (also called Mobile Host MH) refers to a host that changes its point of attachment from one network or subnetwork to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its (constant) IP address. 'Mobile Station (MS)' is a mobile node having a radio interface to the network. A 'Tunnel' is the path followed by a datagram when it is encapsulated. The model is that, while it is encapsulated, a datagram is routed to a known decapsulation agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination. Each mobile node is connected to a home agent over a unique tunnel, identified by a tunnel identifier which is unique to a given Foreign Agent/Home Agent pair.

20 'Home Network' is the IP network to which a user logically belongs. Physically, it can be e.g. a local area network (LAN) connected via a router to the Internet. 'Home Address' is an address that is assigned to a mobile node for an extended period of time. It may remain unchanged regardless of where

the MN is attached to the Internet. Alternatively, it could be assigned from a pool of addresses.

'Mobility Agent' is either a home agent or a foreign agent. 'Home Agent HA' is a routing entity on a mobile node's home network which tunnels packets for delivery to the mobile node when it is away from home, and maintains current location information for the mobile node. It tunnels datagrams for delivery to, and, optionally, detunnels datagrams from, a mobile node when the mobile node is away from home. 'Foreign Agent FA' refers to a routing entity in a mobile node's visited network which provides routing services to the mobile node while registered, thus allowing a mobile node to utilise its home network address. The foreign agent detunnels and delivers packets to the mobile node that were tunnelled by the mobile node's home agent. For datagrams sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

RFC2002 defines 'Care-of Address' (COA) as the termination point of a tunnel toward a mobile node, for datagrams forwarded to the mobile node while it is away from home. The protocol can use two different types of care-of address: a "foreign agent care-of address" is an address announced by a foreign agent with which the mobile node is registered, and a "co-located care-of address" is an externally obtained local address which the mobile node has acquired in the network. An MN may have several COAs at the same time. An MN's COA is registered with its HA. The list of COAs is updated when the mobile node receives advertisements from foreign agents. If an advertisement expires, its entry or entries should be deleted from the list. One foreign agent can provide more than one COA in its advertisements. 'Mobility Binding' is the association of a home address with a care-of address, along with the remaining lifetime of that association. An MN registers its COA with its HA by sending a Registration Request. The HA replies with a Registration Reply and retains a binding for the MN.

A single generic mobility handling mechanism that allows roaming between all types of access networks would allow the user to conveniently move between fixed and mobile networks, between public and private networks as well as between PLMN's with different access technologies. Therefore, mechanisms supporting the Mobile IP functionality are being developed also in mobile communication systems, such as UMTS and GPRS.

It is desired that the Mobile IP will be implemented as an overlay of the UMTS/GPRS network while maintaining backwards compatibility with present systems, assuming minimal modifications in the GPRS standards and on networks whose operators do not want to support MIP. Fig. 1 illustrates the minimum configuration for a GPRS operator, who wishes to offer the mobile IP service. The current GPRS structure is kept and handles the mobility within the PLMN, while MIP allows user to roam between other systems, such as LAN's, and UMTS without losing an ongoing session. In Fig. 1 the foreign agents FA are located at GGSN's. All GGSN's may not have FA's. The SGSN and the GGSN may also be co-located. One FA in a PLMN is sufficient for offering MIP service, but for capacity and efficiency reasons, more than one may be desired. This means that the MS must request a PDP context to be set up with a GGSN that offers FA functionality. While setting up the PDP context, the MS is informed about network parameters of the FA, e.g. care-of address.

The MS may have the same care-of address COA, during a session, i.e. as long as a PDP context is activated. A very mobile MS might perform several inter-SGSN HO's during a long session which may cause an inefficient routing. As an initial improvement, a streamlining procedure, with a temporary anchoring point in the GGSN, could be introduced: If the MN is not transferring data, or possible even in the active state, while moving from one SGSN to another, a new PDP context could be setup between the new SGSN and its associated GGSN at the handover. The MN will get a new care-of address. If the MN is transferring data, e.g. being involved in a TCP session, the MN would move from the old SGSN to the new one while keeping the PDP Context in the old (anchor) GGSN for the duration of the data transfer. Once the data transfer is terminated, the PDP Context can be moved to the GGSN associated with the new SGSN. In other words, a new virtual connection to a new GGSN and an associated FA is established. A typical feature of the mobility agent in the mobile IP is that it periodically transmits agent advertisement messages to the mobile nodes in order to advertise its services. The mobile nodes use these advertisements to determine the current point of attachment to the Internet. In merit of the new connection established by the access node to the new mobility agent, the agent advertisement messages sent by the new mobility agent can be received by the mobile node, and thereby the mobile node is able to detect the change of the attachment point (i.e. mobility agent) and to initiate a standard mobile IP registration.

More generally, in any Mobile IP agent registration, a PDP context is first opened. Then the agent registration is made over the open PDP context.

5 The problem is that because the mobile IP signalling is transferred on the user plane, the underlaying access network nodes, such as the RNC and the SGSN, have no possibility to know whether the registration was successful or not. Thus, if the agent registration procedure fails, the underlaying infrastructure is totally ignorant to the failure. This causes the unused PDP context to remain open and to use the resources unnecessarily. In the inter-  
10 GGSN (or inter-FA) handover described above an additional problem arises. When the handover is performed, the SGSN controlling the handover has no possibility of knowing when closing the connection (PDP context) to the old GGSN/FA.

15 Similar problems may be encountered in any mobility management on a system level overlaying the access network. These various overlaying mobility managements are commonly referred to as a macro mobility management herein.

#### **Disclosure of the Invention**

20 An object of the present invention is to overcome or alleviate the above described problems.

The object is achieved by a method and a system which are characterized by what is disclosed in the attached independent claims. Preferred embodiments of the invention are disclosed in the attached dependent claims.

25 In the present invention the gateway node having the associated (integrated) mobility entity is arranged to monitor the macro mobility registration during an initial registration or during a handover, and to trigger a deletion of any access network protocol context which is no longer necessary on basis  
30 of the result of the registration. For example, the access network protocol context may be deleted, if the registration irrecoverably fails. If the registration is successful but a retry could be successful (the first failure was due to a load situation, for example), the PDP context may not be deleted, but the registration is retried. Mobility entity may be any entity which provides a point of attachment on the macro mobility level, such as a mobility agent in the mobile IP  
35 type mobility management. In the preferred embodiment of the invention the macro mobility management is mobile IP type mobility management.

The present invention avoids the unnecessary use of access network resources after a failed macro mobility registration. It has also an advantage of reduced signalling in comparison to a case where a mobile node/station deletes first the mobile IP entities and then the PDP contexts  
5 some time after the failed registration.

### **Brief description of the Drawings**

In the following, the invention will be described in greater detail by means of preferred embodiments with reference to the accompanying drawings, in which  
10

Figure 1 illustrates GPRS network architecture, and

Figure 2 is a signalling diagram illustrating the method according to the invention,

Figure 3 is a flow diagram illustrating the inventive functionality at the GGSN and the SGSN, and  
15

Figure 4 is a block diagram illustrating the functional blocks of the GGSN involved with the present invention.

### **Preferred Embodiments of the Invention**

The present invention can be applied to any communications requiring a macro mobility management which overlays the mobility management of an access network. The invention suits especially well for supporting a mobile IP type mobility management in an access network. Access network may be any access network, such as a radio access network. The invention  
20 can be especially preferably used for providing a general packet radio service GPRS in the pan-European digital mobile communication system GSM (Global System for Mobile Communication) or in corresponding mobile communication systems, such as DCS1800 and PCS (Personal Communication System), or in third generation (3G) mobile systems, such as UMTS, implementing a GPRS-type packet radio. In the following, the preferred embodiments of the invention  
25 will be described by means of a GPRS packet radio network formed by the GPRS service and the 3G or GSM system without limiting the invention to this particular access system.  
30

A GPRS architecture utilizing a 3G radio access (such as UMTS) or  
35 a 2G radio access (such as GSM) is illustrated in Fig. 1. The GPRS infrastructure comprises support nodes such as a GPRS gateway support node

(GGSN) and a GPRS serving support node (SGSN). The main functions of the GGSN nodes involve interaction with the external data network. The GGSN updates the location directory using routing information supplied by the SGSNs about an MS's path and routes the external data network protocol packet encapsulated over the GPRS backbone to the SGSN currently serving the MS. It also decapsulates and forwards external data network packets to the appropriate data network and handles the billing of data traffic.

The main functions of the SGSN are to detect new GPRS mobile stations in its service area, handle the process of registering the new MSs along with the GPRS registers, send/receive data packets to/from the GPRS MS, and keep a record of the location of the MSs inside of its service area. The subscription information is stored in a GPRS register (HLR) where the mapping between a mobile's identity (such as MS-ISDN or IMSI) and the PSPDN address is stored. The GPRS register acts as a database from which the SGSNs can ask whether a new MS in its area is allowed to join the GPRS network.

The GPRS gateway support nodes GGSN connect an operator's GPRS network to external systems, such as other operators' GPRS systems, data networks 11, such as an IP network (Internet) or a X.25 network, and service centres. Fixed hosts 14 can be connected to data network 11 e.g. by means of a local area network LAN and a router 15. A border gateway BG provides an access to an inter-operator GPRS backbone network 12. The GGSN may also be connected directly to a private corporate network or a host. The GGSN includes GPRS subscribers' PDP addresses and routing information, i.e. SGSN addresses. Routing information is used for tunnelling protocol data units PDU from data network 11 to the current switching point of the MS, i.e. to the serving SGSN. The functionalities of the SGSN and GGSN can be connected to the same physical node (SGSN+GGSN).

The home location register HLR of the GSM network contains GPRS subscriber data and routing information and it maps the subscriber's IMSI into one or more pairs of the PDP type and PDP address. The HLR also maps each PDP type and PDP address pair into a GGSN node. The SGSN has a Gr interface to the HLR (a direct signalling connection or via an internal backbone network 13). The HLR of a roaming MS and its serving SGSN may be in different mobile communication networks.



The intra-operator backbone network 13, which interconnects an operator's SGSN and GGSN equipment can be implemented, for example, by means of a local network, such as an IP network. It should be noted that an operator's GPRS network can also be implemented without the intra-operator backbone network, e.g. by providing all features in one computer.

Network access is the means by which a user is connected to a telecommunication network in order to use the services and/or facilities of that network. An access protocol is a defined set of procedures that enables the user to employ the services and/or facilities of the network. The SGSN, which is at the same hierarchical level as the mobile switching centre MSC, keeps track of the individual MSs' location and performs security functions and access control. GPRS security functionality is equivalent to the existing GSM security. The SGSN performs authentication and cipher setting procedures based on the same algorithms, keys, and criteria as in existing GSM. GPRS uses a ciphering algorithm optimised for packet data transmission.

In order to access the GPRS services, a MS shall first make its presence known to the network by performing a GPRS attach. This operation establishes a logical link between the MS and the SGSN, and makes the MS available for SMS over GPRS, paging via SGSN, and notification of incoming GPRS data. More particularly, when the MS attaches to the GPRS network, i.e. in a GPRS attach procedure, the SGSN creates a mobility management context (MM context), and a logical link LLC (Logical Link Control) established between the MS and the SGSN in a protocol layer. MM contexts, are stored in the SGSN and MS. The MM context of the SGSN may contain subscriber data, such as the subscriber's IMSI, TLLI and location and routing information, etc.

---

In order to send and receive GPRS data, the MS shall activate the packet data address that it wants to use, by requesting a PDP activation procedure. This operation makes the MS known in the corresponding GGSN, and interworking with external data networks can commence. More particularly, one or more PDP context is created in the MS and the GGSN and the SGSN, and stored in the serving SGSN in connection with the MM context. The PDP context defines different data transmission parameters, such as the PDP type (e.g. X.25 or IP), PDP address (e.g. IP address), quality of service QoS and NSAPI (Network Service Access Point Identifier). The MS activates the PDU context with a specific message, Activate PDP Context Request, in which it

gives information on the TLLI, PDP type, PDP address, required QoS and NSAPI, and optionally the access point name APN. The SGSN send a create PDP context message to the GGSN which creates the PDP context and send it to SGSN. SGSN sends the PDP context to MS in a Activate PDP Context  
 5 Response message, and a virtual connection or link between the MS and the GGSN is established. As a result the SGSN forwards all the data packets from the MS to the GGSN, and the GGSN forwards the SGSN all data packets received from the external network and addressed to the MS. The PDP context is stored in the MS, the SGSN and the GGSN. When the MS roams to the  
 10 area of a new SGSN, the new SGSN requests MM and PDP contexts from the old SGSN.

Fig. 1 illustrates the implementation of mobile IP in the GPRS/3G environment.

The MS can be a laptop computer PC connected to a packet radio  
 15 enabled cellular telephone. Alternatively, the MS can be an integrated combination of a small computer and a packet radio telephone, similar in appearance to the Nokia Communicator 9000 series. Yet further embodiments of the MS are various pagers, remote-control, surveillance and/or data-acquisition devices, etc. The user of a mobile station MS subscribes to a special Mobile IP  
 20 service. The subscription information is stored in the Home Location Register HLR together with the user's home IP address.

In Fig. 1 the foreign agents FA are located at (integrated into) GGSN's. An alternative is that the SGSN and the GGSN are co-located, and the FA's are located at SGSN+GGSNs. The present invention is applicable in  
 25 both cases. It should be noted that there may be more than one SGSN and GGSN in one network. All GGSN's may not have FA's. Each FA has an IP address in the Internet and in the operator's own private GPRS/3G backbone network. More precisely, the FA's IP address is such that IP packets destined to that address are routed in the Internet to the GGSN associated with the FA.  
 30 When the MN leaves its home subnet and registers to a new FA, it can no longer be reached on the basis of its home IP address alone, but must be assigned an address belonging to the visited network, called the *care-of address* (COA). The care-of address positively identifies the instantaneous location of the mobile terminal and may be: 1) the IP address of the FA belonging to the  
 35 visited network, or 2) an IP address acquired directly by the mobile terminal through an autoconfiguration mechanism from the local IP address space, in

which case the term co-located care-of address is used. When registering to a new FA and obtaining a COA, the MN which when registers with a home agent HA, in its home network, informing the latter of its COA. In Fig. 1 a home agent HA is located in a data network 11 which is the home network of the mobile node MN associated with the mobile station MS. A second host 14 wishing to communicate with the MN need not to be aware of the MN has moved: it simply sends IP packets addressed to MN's home IP. address. These packets are routed via normal IP routing to the MN's home network, there they are intercepted by the HA. The HA encapsulates each such packet in another IP packet which contains the MN's COA as these packets are thus delivered to the FA (a process called tunneling). The FA forwards the IP packet to the GGSN. The GGSN forwards the IP packet (which may be encapsulated for transmission over the GPRS backbone) to the serving SGSN which further forwards the IP packet to the MS/MN. Packets from the MN to the another host 14 need not necessarily be tunneled: the MN may simply send them to the GGSN which directly forwards the packets to the second host 14, without interception by the FA or the HA.

An example of inter-GGSN handover will be now described with reference to Figure 2.

A reference is now made to Figure 1. The home network of the mobile station MS is the GPRS/3G network 1. The user of the mobile station MS subscribes to a special mobile IP service, and an IP application in the MS or in a separate data terminal is a mobile node MN in a mobile IP communication. It is assumed that the MS/MN is attached to the home network 1 and the radio access network RAN1 (PS1 and PSC/RNC1). A serving support node in the home network is SGSN1. MM and PDP contexts have been created for mobile IP service as described above, and a virtual connection is provided between MS/MN and SGSN1 as well as between the SGSN1 and a gateway node GGSN1 which has an associated foreign agent FA1. Thus, the IP packets addressed to the MN can be forwarded to the MN over the home network 1 and RAN1. The COA of the MN has been registered to the home agent HA in the home network 11 of the MN, so that a mobile IP tunnelling is provided from the HA to the GGSN/FA1.

Let us now assume that the MS/MN moves to service area of another GPRS/3G network 2 which is served by a support node SGSN2. When the MS/MN arrives at a new RAN2, the MS part listens to radio broadcast

messages, which contain information about radio parameters, network and cell identity, etc. as well as e.g. information about available core network, service providers, service capabilities etc. On the basis of the broadcast the MS determines that the network and/or the routing area has changed. Upon detecting a change of routing area, the MS/MN sends a routing area update request to the new SGSN, namely SGSN2, as shown in Figure 2. The new SGSN2 sends a SGSN context request message to the old SGSN1 (at step 2) to get the MN and PDP contexts for the MS/MN. The old SGSN1 responds with a SGSN context response message which contain the MN and PDP contexts (step 3). According to the preferred embodiment of the invention, the In an embodiment of the invention, the information transferred from the old access node to the access node may be provided with an information field which indicates the different types of the PDP contexts, or at least the Mobile IP related PDP contexts. This allows the SGSN to distinguish the Mobile IP dedicated PDP contexts from other active PDP contexts of the mobile station which should not be involved with the change of the mobility agent. There are various possible ways to implement the PDP context type information. For example, a PDP Context Information Element, which is carried in the SGSN Context Response message in the GPRS (and in forward SNRC relocation message in UMTS) may be provided with a field indicating the type of service used over the PDP context. The type field may contain an access Point Name which has a value indicating a Mobile IP PDP context. Spare bits in the PDP Context Information Element may be used for the new field, or alternatively the new field may an extension of the current PDP Context Information Element format. It should be noted, however, that the exact implementation is not relevant to the invention. It is only relevant, in this specific embodiment, that the information received from the old SGSN enables the new SGSN to determine which one(s) of the PDP contexts is (are) dedicated to the Mobile IP.

At step 4 the new SGSN2 may, in certain situations, execute authentication/security functions which may involve an interrogation to the HLR of the MS/MN. If the user has at least one activated PDP context, when the new SGSN2 sends a SGSN context acknowledge message to the old SGSN1. The old SGSN1 may now start forwarding of buffered data packets belonging to the activated PDP context, if any, to the new SGSN2. The new SGSN2 now detects that new foreign agent FA2 should be preferably used instead of FA1, at step 6. The SGSN2 deletes the PDP context in the old

GGSN/FA1 by sending a delete PDP context requests to the old GGSN/FA1. As a result any active PDP context in the GGSN/FA1 is deactivated, and the GGSN/FA1 acknowledges by sending a delete PDP context response to the new SGSN2 (step 8 in Figure 2). Referring again to Figure 3, the process proceeds to the step 34 wherein the new SGSN2 creates a PDP context in the GGSN/FA2 by sending a create PDP context requests to the new GGSN/FA2 (step 9 in Figure 2). The GGSN/FA2 creates the PDP context for the MS/MN and returns a create PDP context response to the new SGSN2 (step 10 in Figure 2). The new SGSN2 establishes MN and PDP context for the MS/MN, and responses to the MS/MN with routing area update accept message (step 11). The MS/MN acknowledges with a routing area update complete message (step 12). A virtual connection has thus been established between the MS/MN and the GGSN/FA2.

All the previous procedures have been executed in the GPRS/3G layer only. Due to the newly established connection to the GGSN/FA2 the MN is able to hear the agent advertisement messages broadcasted by the new FA2 in accordance with the mobile IP protocol. Upon receiving the agent advertisement from the new FA2, the MN is able to detect a change in point of attachment, i.e. change of FA, in accordance with the MIP standard. The agent advertisement message may also include the care-of-address COA, or the MN may acquire the COA in accordance with the MIP standard. Then the mobile node MN registers its COA with its home agent HA in accordance with the MIP standard (step 14 in Figure 2). Depending on its method of attachment, the MN will register either directly with its HA, or through the new FA which forwards the registration to the HA. Thereafter, the mobile IP tunnelling between the HA and the old GGSN/FA1 is released and the new mobile IP tunneling is established between the HA and the new GGSN/FA2, in accordance with the mobile procedures.

As the mobile IP signalling is transferred on the user plane, the underlying access network nodes, such as the RNC and the SGSN, have no possibility to know whether the registration was successful or not.

According to the present invention the GGSN2 monitors (step 15) whether the Mobile IP registration is successful or fails. This is possible since the FA2 is located at the GGSN2, and therefore, the GGSN2 also knows the status of the FA2. When the GGSN2 detects that the registration is successful, no further measures are required except that the old connection between

GGSN1 and SGSN2 must be deleted. However, if the GGSN2 detects that the registration fails, the GGSN2 can determine the severity of the failure and decide whether it should allow the mobile node MN to try to register again or if the registration procedure should be terminated and the PDP context deleted.

- 5 If the GGSN decides that the registration can be tried again, the PDP context is maintained. If the GGSN2 decides that the failure is that severe that no repetition of the registration procedure cannot be allowed in order to complete the registration, the GGSN2 deletes the associated PDP context at the GGSN2 (step 16) and sends to the SGSN2 a Delete PDP message to the
- 10 SGSN2 (step 17). The message may also include a cause value which indicates why the deletion was made, i.e. failure in the MIP registration. The SGSN2 receives the message and deletes the PDP context to the GGSN2 (step 18). The SGSN2 may also use the cause value in the message in deciding (step 19) whether the other PDP context open to the old GGSN1
- 15 (assuming the steps 7 and 8 have not yet been performed) should be maintained or deleted, or should also the Air PDP context to the MS/MN be deleted. If the PDP context to the old GGSN1 is maintained, the MS/MN is able to reregister to the FA1 and/or continue communication. To enable this alternative, the deletion of the old PDP context, i.e. steps 7 and 8, is delayed long
- 20 period of time that a possible Delete PDP message from the GGSN2 due to a failed registration will be received before the deletion. At step 20, SGSN2 sends Delete PDP Request messages to MS and GGSN1, upon deciding that PDP contexts are to be deleted both in the MS and GGSN1.

- The principles described above are applicable to any situation in
- 25 which a MIP registration is attempted. In the GPRS attach procedure the MS requests a PDP activation for mobile IP by an Activate PDP Context Request message. The SGSN2 sends a Create PDP Context message to the GGSN2 which creates the PDP context and send it to SGSN2. SGSN2 sends the PDP context to MS in a Activate PDP Context Response message. Thus, a PDP
- 30 context is created in the MS and the GGSN2 and the SGSN2 and a virtual connection or link between the MS and the GGSN2/FA2 is established. As a result, a MIP registration can be now performed over the virtual connection. As described above with respect Fig. 2, the GGSN2 monitors the Mobile IP registration procedure and deletes the PDP context and releases the virtual
- 35 connection, if the registration fails.

Figure 3 is a flow diagram illustrating the inventive functionality at the GGSN and the SGSN. First, at step 31 a PDP context and a new connection is created. Then a MIP registration is attempted over a new connection (step 32). The GGSN monitors the registration (step 33) and determines  
 5 whether the registration was successful or not (step 34). If the registration was successful the GGSN determines whether there are other MIP-PDP contexts for the mobile node MN. If not, the procedure is ended. If there is another MIP-PDP context which is unnecessary the new registration, the unnecessary PDP context is deleted (step 43) and the procedure is ended.

10 However, if it is determined in the step 34 that the registration fails, it is then determined whether it is possible to retry the registration (step 35). If yes, the registration is retried (step 36) and the procedure returns to the step 33. If the retry is not possible, the PDP context is deleted at the GGSN and a deleted PDP context message with a cause value is sent to the SGSN (step  
 15 37). The SGSN determines whether there is other PDP context(s) for the same MN (step 38). If not, the connection to the MN, and the old GGSN/FA is deleted (step 41). If any other PDP context exists in step 38, it is checked whether a fallback to this old PDP context is possible (step 39). If not, the procedure proceeds to step 41. If the fallback is possible in step 39, the old PDP  
 20 context to the old FA and the old FA is used (step 40).

Figure 4 is a block diagram illustrating the functional blocks of the GGSN involved with the present invention. Firstly, a macro mobility management entity 41, such as the foreign FA, is integrated into the GGSN. Further, monitoring means 42 are provided for monitoring the macro mobility (MIP)  
 25 registration. The determining means 53 are provided for determining on basis of the result of the monitored registration whether there is at least one unnecessary PDP context. Triggering means 54 are responsive to the determining means 45 so as to trigger a deletion of any determined unnecessary PDP context. The PDP context deletion means stand for any entity or functionality  
 30 in the system which is required for deleting a PDP context.

The description only illustrates preferred embodiments of the invention. The invention is not, however, limited to these examples, but it may vary within the scope and spirit of the appended claims.

## Claims

1. A method of managing access network protocol context in an access system comprising a plurality of mobile nodes (MS/MN), access nodes (SGSN1, SGSN2) serving said mobile nodes, a first gateway node (GGSN1) for interfacing said first part (RAN1) of the access system with external networks (12), and a first mobility entity (FA1) which is associated with said first gateway node (GGSN1) and arranged to provide macro mobility management services to the mobile nodes (MS/MN) while registered to a respective part (RAN1) of the access system, said method comprising steps of
  - opening at least one access network protocol context at a first access node and the first gateway node in order to establish a connection between one of said plurality of mobile nodes (MS/MN) and said first gateway node
  - initiating a macro mobility registration over said access network connection between the mobile node and the first mobility entity, characterized by further steps of
    - monitoring at the first gateway node the macro mobility registration, determining on the basis of the result of the registration that at least one access network protocol context is no longer necessary,
    - triggering a deletion of the unnecessary access network protocol context.
2. The method as claimed in claim 1, characterized by determining at the first gateway node, in response to detecting a failure in said macro mobility registration, whether it is possible to retry the macro mobility registration or whether the registration has irrecoverably failed.
- ~~3. The method as claimed in claim 1 or 2, characterized by the gateway node sending a context deletion message to the first access node, when the macro mobility registration irrecoverably fails.~~
4. The method as claimed in claims 3, characterized by deleting at the first access node the PDP context to the first gateway node in response to receiving said context deletion message.
5. The method as claimed in claims 4, characterized by deleting at the first access node the PDP context to the mobile node in response to receiving said deletion message.



6. The method as claimed in any one of claims 1-5, characterized by said registration being due to an handover from a second gateway node to said first gateway node, the method comprising further steps of

deciding at the first access node, in response to receiving a context  
 5 deletion message from the first gateway node, whether to maintain or recreate an old PDP context to an old gateway node, or to delete the PDP context to the old gateway node and/or to the mobile node.

7. The method as claimed in claims 6, characterized by  
 said decision being based on a cause value in said context deletion  
 10 message, said cause value indicating a cause of sending the context deletion message.

8. The method according to any one of claims 1-7, characterized in that said macro mobility management is Internet Protocol-type, or IP type mobility management.

15 9. The method as claimed in any one of claims 1-8 in a radio access system, characterized in that said access network protocol context comprises a packet protocol context .

10. The method as claimed in any one of claims 1-9, characterized in that said mobility entity associated with the a gateway node  
 20 (GGSN2) is a foreign agent (FA2).

11. An access system, comprising  
 a plurality of mobile nodes (MS/MN),  
 access nodes (SGSN1,SGSN2)  
 a first gateway node (GGSN1) for interfacing said access system  
 25 with external networks (11),

a first mobility entity (FA1) which is associated with said first gateway node (GGSN1) and arranged to provide macro mobility management services to the mobile nodes (MS/MN) while registered to a respective part (RAN1) of the access system,

30 each mobile node being able to perform a macro mobility registration to the first mobility entity over a respective dedicated access network connection established by opening an access network protocol context at a first access node and the first gateway node characterized by

the first gateway node being arranged to monitor the macro mobility  
 35 registration, to trigger a deletion of any access network protocol context which is no longer necessary on basis of the result of the registration.

12. The system as claimed in claim 11, characterized by the first gateway node being arranged to determine, in response to detecting a failure in said macro mobility registration, whether it is possible to retry the macro mobility registration or whether the registration has irrecoverably failed.

13. The system as claimed in claim 11 or 12, characterized by the gateway node being arranged to send a context deletion message to the first access node, when the macro mobility registration irrecoverably fails.

14. The system as claimed in claims 13, characterized by the first access node being arranged to delete the PDP context to the first gateway node and/or the PDP context to the mobile node in response to receiving said deletion message.

15. The system as claimed in any one of claims 11-14, characterized by said registration being due to an handover from a second gateway node to said first gateway node, and said first access node being arranged to decide, in response to receiving a context deletion message from the first gateway node, whether to maintain or recreate an old PDP context to an old gateway node, or to delete the PDP context to the old gateway node and/or to the mobile node, based on a cause value in said context deletion message, said cause value indicating a cause of sending the context deletion message.

16. The system as claimed in any one of claims 11-15, characterized in that said macro mobility management is Internet Protocol type, or IP type mobility management, and in that said mobility entity associated with the a gateway node (GGSN2) is a foreign agent (FA2).

17. The system as claimed in any one of claims 11-16 in a radio access system, characterized in that said access network protocol context comprises a packet protocol context.

18. A gateway node for an access system which comprises a plurality of mobile nodes (MS/MN), access nodes (SGSN1,SGSN2) and a first mobility entity (FA1) which is associated with said first gateway node (GGSN1) and arranged to provide macro mobility management services to the mobile nodes (MS/MN), each mobile node being able to perform a macro mobility registration to the first mobility entity over a respective dedicated access network connection established by opening an access network protocol context at a first access node and the first gateway node characterized by said

the first gateway node being arranged to monitor the macro mobility registration and to trigger a deletion of any access network protocol context which is no longer necessary on basis of the result of the registration.

19. The gateway node as claimed in claim 18, characterized  
5 by said gateway node being arranged to determine, in response to detecting a failure in said macro mobility registration, whether it is possible to retry the macro mobility registration or whether the registration has irrecoverably failed.

20. The gateway node as claimed in claim 18 or 19, characterized  
10 by said gateway node being arranged to send a context deletion message to the first access node, when the macro mobility registration irrecoverably fails.

21. The gateway node as claimed in claim 18, 19 or 20, characterized  
by said gateway node being integrated into same physical node  
with said access node.

**(57) Abstract**

In an access network which supports a mobile IP protocol, a packet data protocol (PDP) context is opened at an support node (SGSN) and a gateway node (GGSN) in order to establish a connection between a mobile node (MS/MN) and a mobile IP foreign agent (FA) located at the gateway node. A mobile IP registration over the connection is initiated. The gateway node (GGSN) monitors (15) whether the registration is successful or fails. The PDP context is deleted (16-18), if the registration irrecoverably fails. If the registration is successful but a retry could be successful (the first failure was due to a load situation, for example), the PDP context may not be deleted, but the registration is retried.

(Fig. 2)

Fig. 1

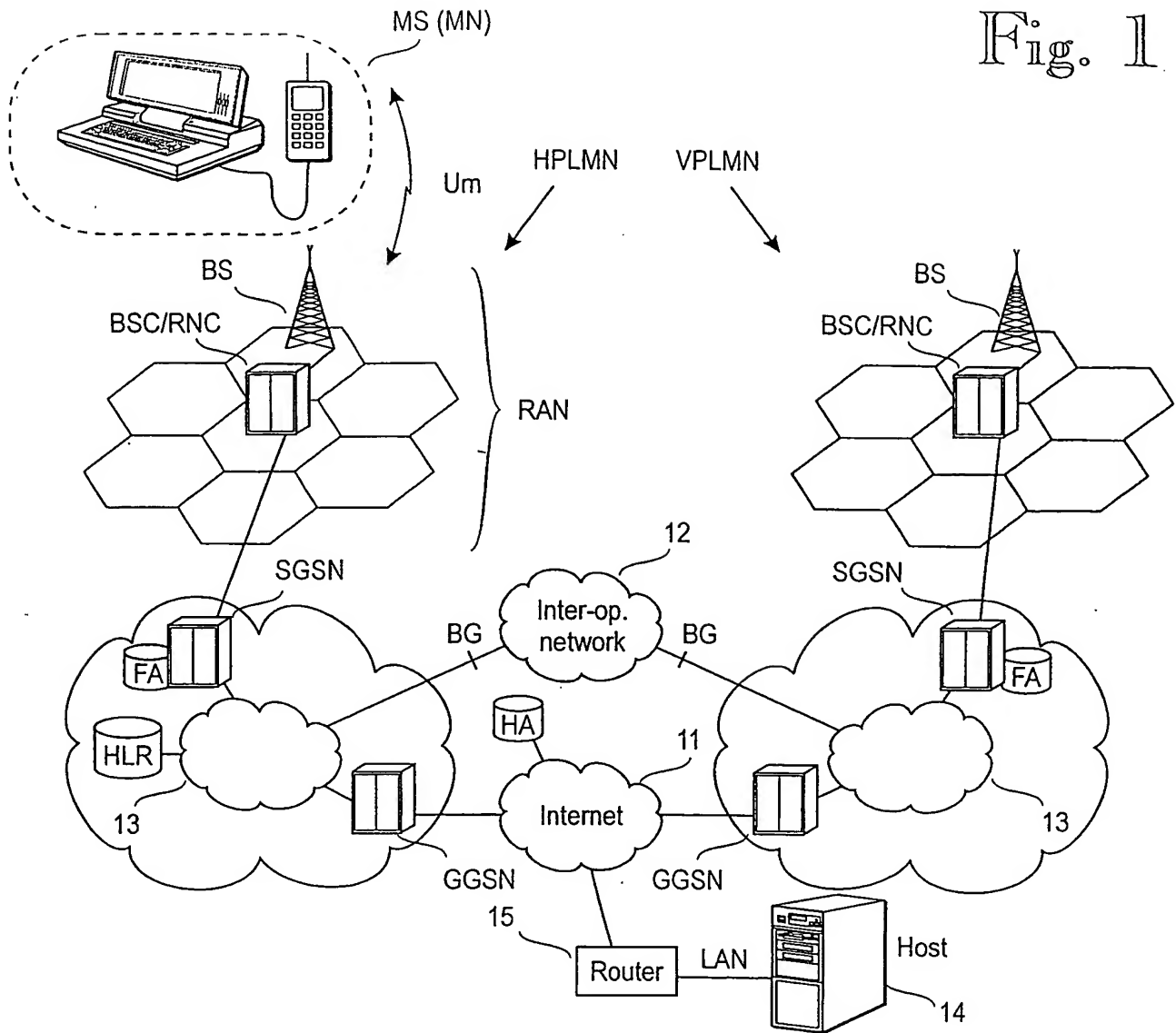
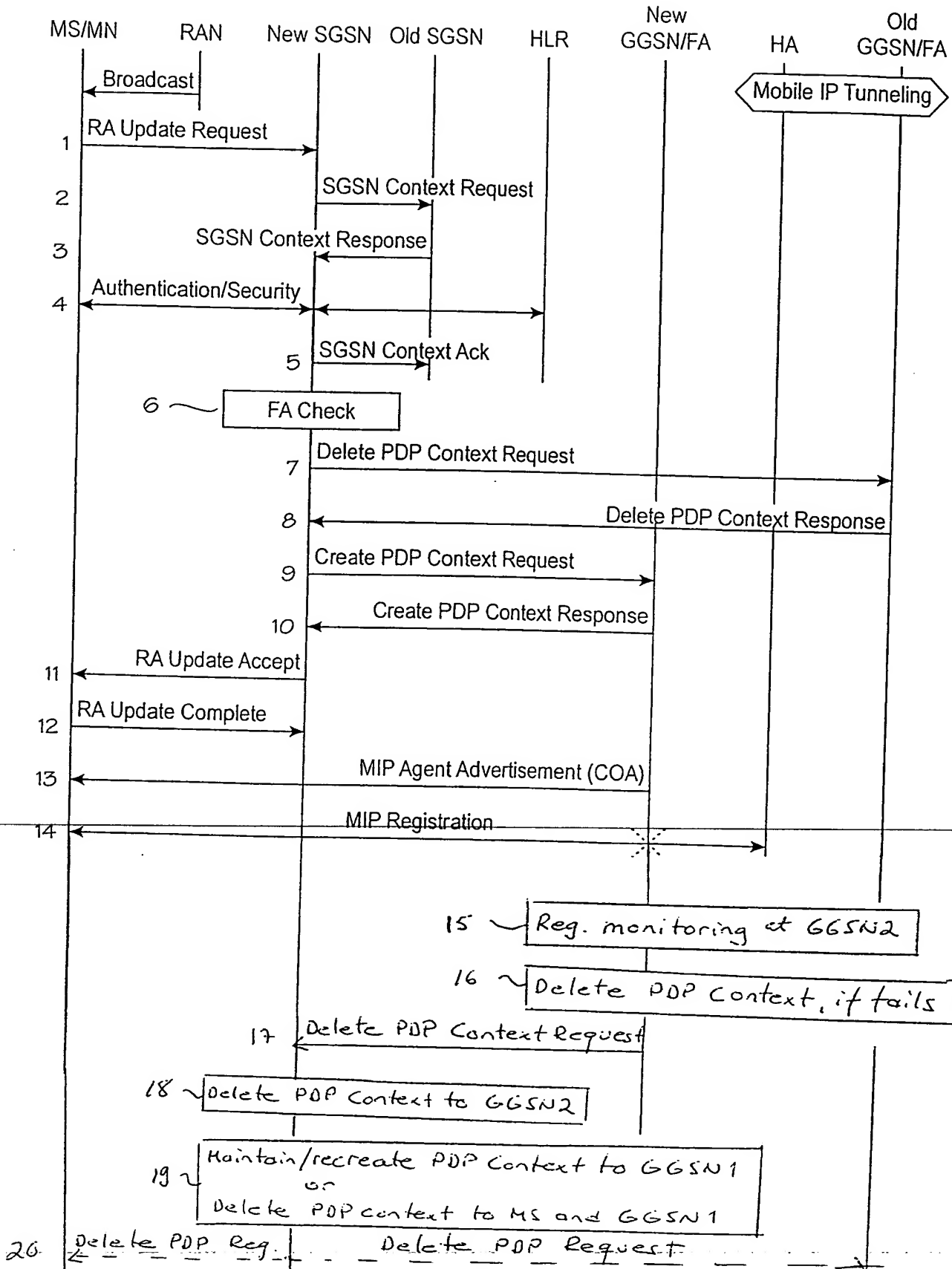


Fig. 2



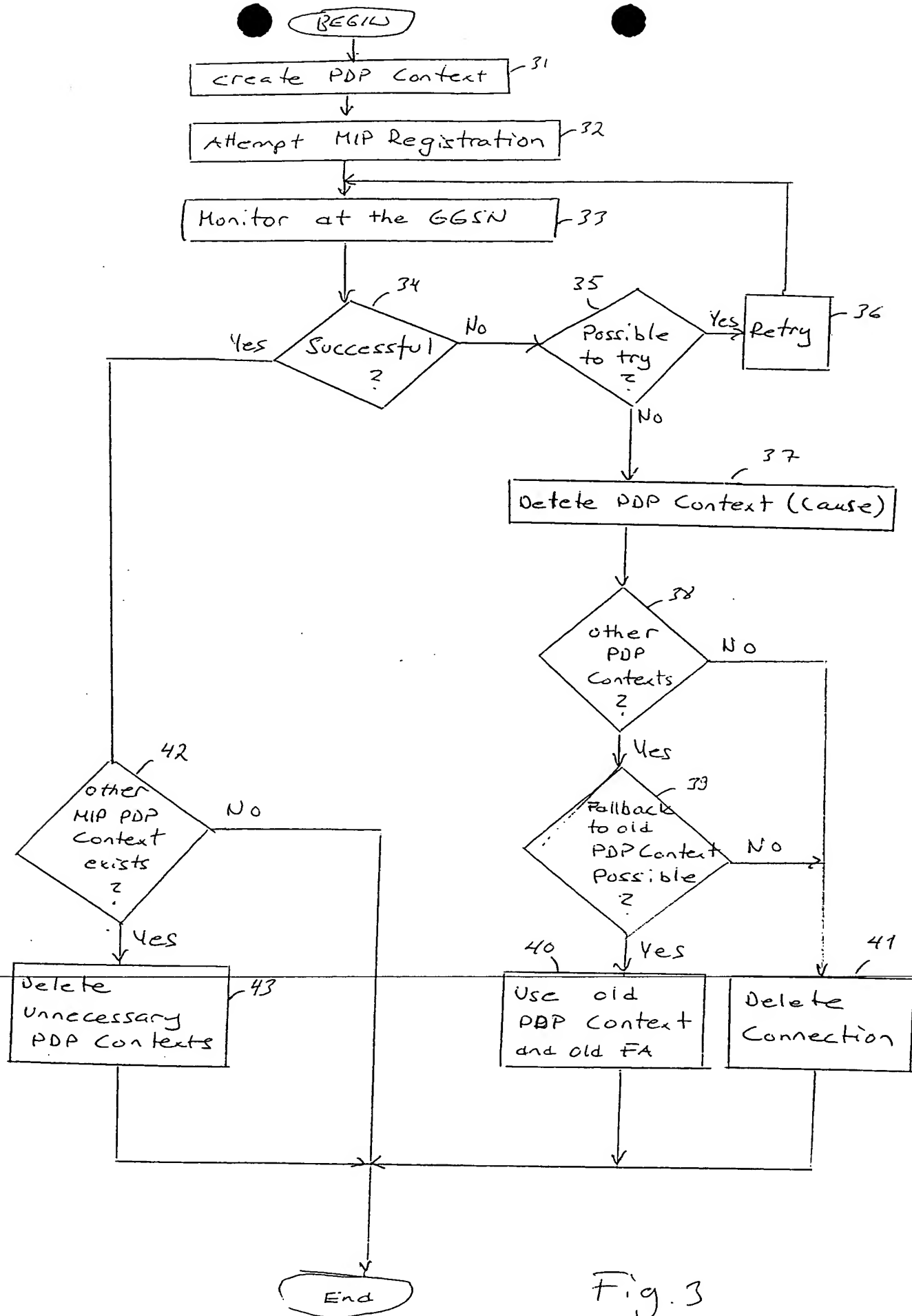


Fig. 3

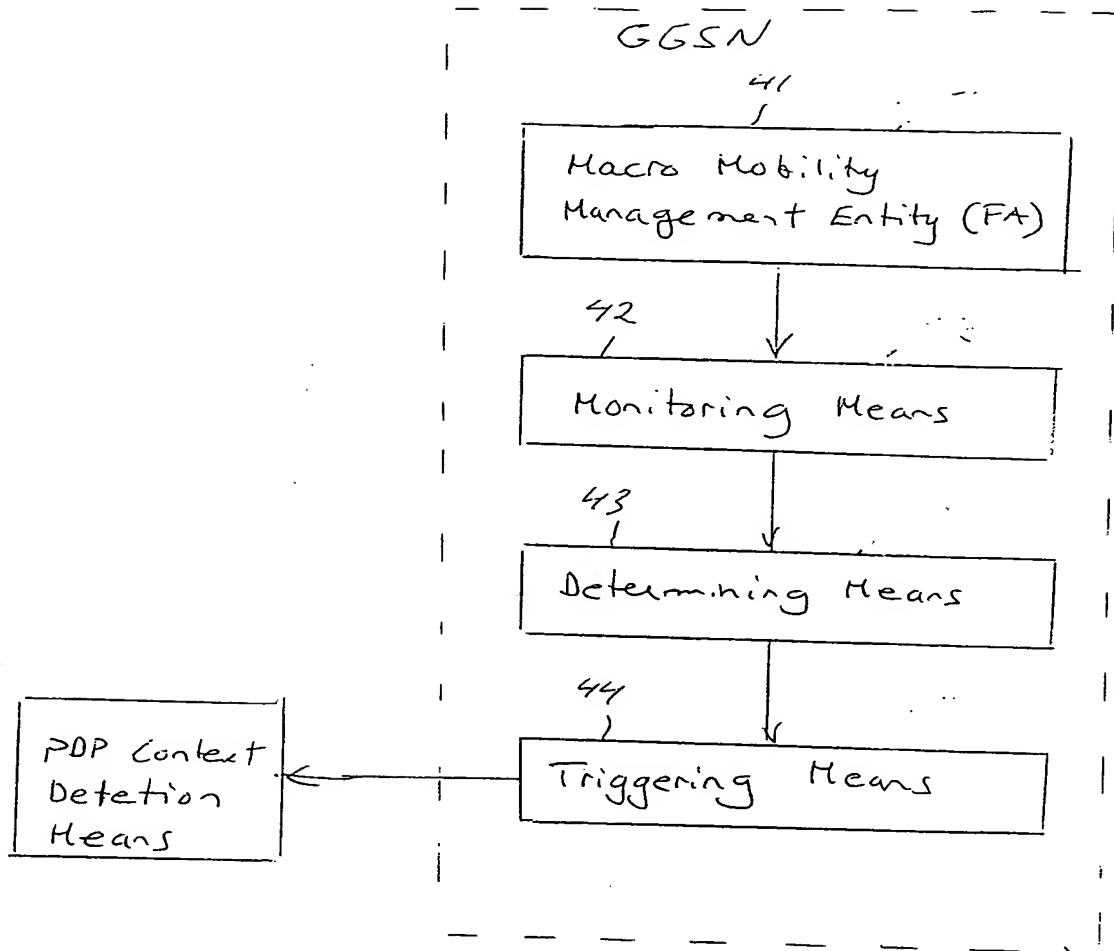


Fig. 4.